SPECIFICATION AMENDMENTS

Please replace the Abstract with the following amended/substitute Abstract.

~~In order to provide a processor for encrypting and/or decrypting data and a method of encrypting and/or decrypting data using such a processor, which are characterized by a lower storage requirement and greater safety against attacks on the rounding key generation than previously known and which are preferably embodied as, respectively, an AES coprocessor and a method of AES calculation, it is provided that a~~ A control device ~~(12)~~ is connected to at least one encryption/decryption ~~means (14)~~ device via at least one communication ~~means (16)~~ device., ~~the~~ The control device ~~(12)~~ is connected to ~~at least one rounding~~ a round key ~~generation means (18)~~ generator via at least one further communication ~~means (20)~~ device., ~~the~~ The control device ~~(12)~~ has at least one external key input ~~(22)~~, the at least one encryption/decryption ~~means (14)~~ device has at least one external data input ~~(24)~~ and at least one external data output ~~(26)~~, and the at least one encryption/decryption ~~means (14)~~ device and the ~~at least one rounding~~ round key ~~generation means (18)~~ generator are decoupled from one another. ~~The method according to the invention provides that at least one initial key is read into a control device, external data are read into at least one encryption/decryption means, at least one data word needed to calculate at least one rounding key is read from at least one storage means of the control device and transferred to at least one~~

~~rounding key generation means, at least one rounding key is calculated recursively on the basis of the at least one data word by means of the at least one rounding key generation means, transferred to the control device and stored in the at least one storage means, the at least one rounding key is transferred to the at least one encryption/decryption means, the external data are encrypted or decrypted by means of the at least one encryption/decryption means using the at least one rounding key and the encrypted or decrypted data are made available at least one external data output, and these steps are repeated as often as necessary to encrypt or decrypt a set of external data.~~